智能路由器

使用手册

A 类设备声明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰，在这种情况下，可能需要用户对其干扰采取切实可行的保护措施。

执行标准:Q/LK 001

说明书声明

此说明书适用于(R2005G、 RA1055)等型号的路由器，如果您发现说明书上的功能比您使用的路由器功能有出入，属于正常情况，一切功能以出厂软件为准。

目 录

1. 认识宽带路由器

1.1. 物品清单

有线路由器 *1

电源线/或外置电源适配器 *1

一对用于安装在机架上的耳片及对应螺丝、垫脚（仅限机架式）

快捷操作指南 *1

请仔细核对你的包装，若有缺少请及时和当地经销商联系。

1.1. 安装环境

路由器应放置于平坦表面，干燥、灰尘少、通风、常温下的环境

1.2. 硬件规格

连接类型： 5 类或 6 类双绞线

协议： IEEE802.3、 IEEE802.3u

工作温度： 0℃～50℃

工作湿度： 10%～90% 非凝结

额定电源： AC 100-240V

1.3. 指示灯说明

指示灯	描述	功能	
PWR	电源灯	常灭	电源未通
		常亮	电源供电正常
CPU	系统指示灯	常灭	系统未启动
		闪烁	只在恢复默认期间出现
		常亮	系统已启动
WAN	WAN 口指示灯	常亮	连接正常
		闪烁	正在传输数据
		常灭	WAN 未连接
WLAN	无线指示灯	闪烁	无线开启
		常灭	无线关闭
LAN/监控	LAN 口/监控口指示灯	常亮	LAN 口连接正常
		闪烁	正在传输数据
		常灭	LAN 口未连接

1.4. 接口、按钮说明

描述	功能
PWR 端口	连接到电源
LAN 端口	连接电脑或者交换机等
监控端口	监控网络专用端口
WAN 端口	用于连接互联网、 ISP 端
Default	恢复默认按钮，在路由器正常工作时用尖状物（如铅笔）按压此按键直到 CPU 快速闪烁后（约为 5 秒左右），松开即可。

2. 监控路由器功能说明

如图：

各 LAN 口和监控口相互隔离，不可以互通，分别对应不同 VLAN，不同业务网段（关于监控业务网段相关设置参见第 6 章内网配置）

上行或下行带宽拥塞时，路由器会优先保证监控口数据带宽（此功能要求必须开启智能 Qos, 并正确设置上下行带宽， 参见第 9 章说明）

特殊情况下，默认业务网段 PC 需访问监控网段设备，可以 PC 创建 VPN 连接的方式访问到监控网段设备，可以参考说明书结尾附录一

3. 安装路由器流程

3.1. 安装流程

注意：“*设置你的计算机” 这一步骤根据使用操作系统不同分为“Windows XP、Vista/Win7”两个部分，请根据你的操作系统选择适合章节阅读。

所有安装步骤请遵循安装流程，避免安装失败。

3.2. 正确连接路由器的接口

(1) 把电源或电源线一端接到路由器的 PWR 接口中，另一端正确接入市电。

(2) 把可以连接因特网的网线接到路由器的 WAN 口，连接电脑的网线接到 LAN 的任意端口，监控网络接入监控口。

连接好后，检查 PWR 指示灯及对应的 LAN， 监控.WAN 的指示灯是否点亮。

小提示：外网线包括 ADSL 猫/光纤猫接出的网线，或者互联网运营商（如电信，联通，移动，长宽等）直接拉进户的网线 。

3.3. 设置你的计算机

说明：将你电脑的 IP 地址和 DNS 均设置为自动获取，用网线连接网卡与路由器的 LAN 口，网卡即能立刻获取 IP 地址，以便进入路由器 Web 配置界面。详细说明见本章节,如果你已经设置好了，则可以跳过这一章节，直接看 2.4 章节。

3.3.1 设置你的计算机（Windows XP）

请按照下述步骤来配置你的电脑

(1) 在桌面上找到网上邻居图标，鼠标右键点击，选择属性。

(2) 选择本地连接，右键点击属性

(3) 点击选择 Internet 协议（TCP/IP），再点击属性按钮

(4) 选择自动获得 IP 地址和自动获得 DNS 服务器地址，然后点击确定，关闭 Internet 协议（TCP/IP）属性窗口

(5) 点击确定，关闭本地连接属性窗口后生效

3.3.2 设置你的计算机（Windows Vista/Windows 7）

请按照下述步骤配置你的电脑

(1) 开始－控制面板

(2) 点击网络和共享中心

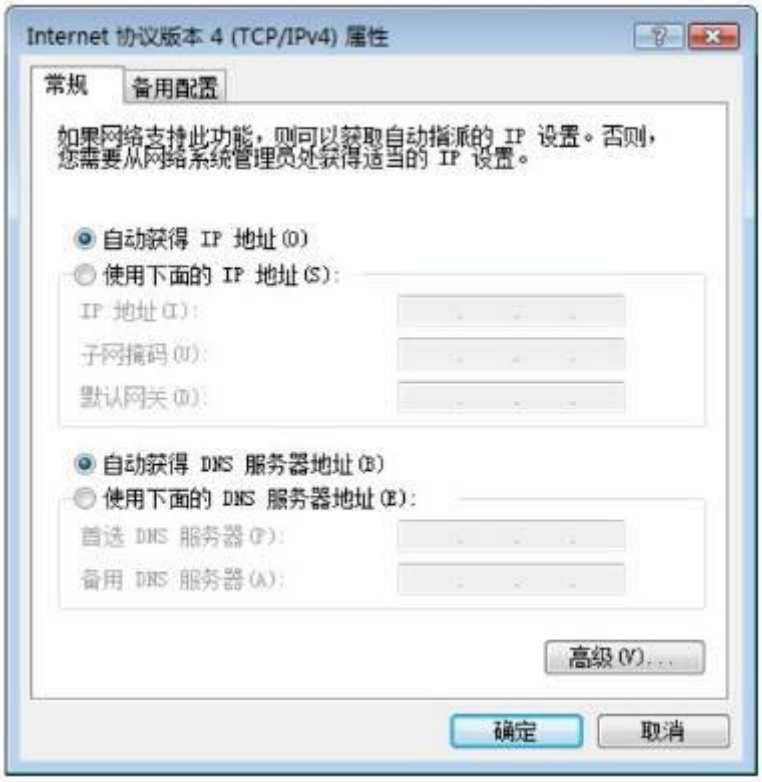
(3) 点击窗口最左边的管理网络连接

以上步骤可以由“按下键盘的 WIN+R 键，在运行里输入 ncpa.cpl，确定后打开“代替”。

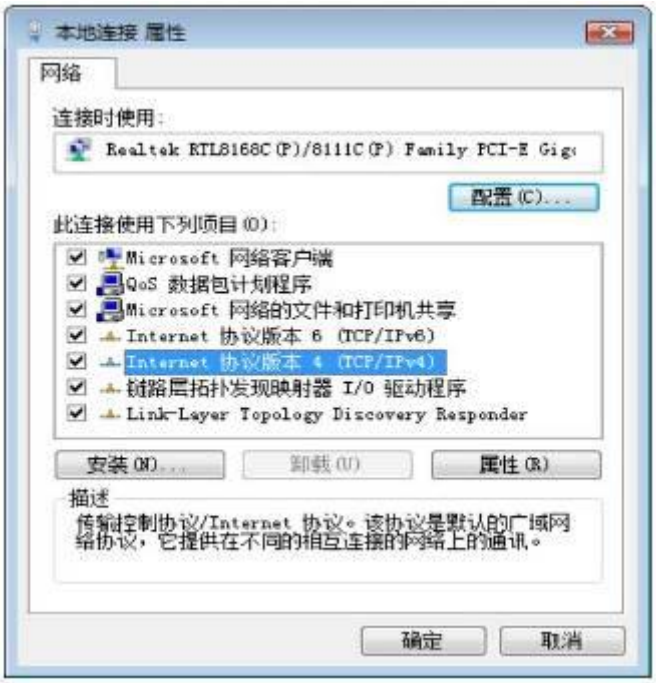
(4) 右键点击本地连接，点击属性

(5) 点击 Internet 协议版本 4（TCP/IP），然后点击属性按钮

(6) 选择自动获得 IP 地址和自动获得 DNS 服务地址，然后点击确定关闭 Internet 协（TCP/IP）属性窗口

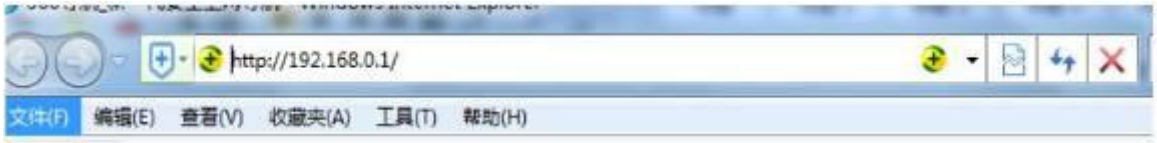


(7) 点击确定关闭本地连接属性窗口



3.4. 登陆路由器设置界面

(1) 打开桌面上的 Internet Explorer 浏览器或其他用来上网的浏览器（如 Opera、 Firefox 等），在地址栏里输入 192.168.0.1 点击 Enter（键盘回车键）。



(2) 在弹出窗口输入用户名： guest 密码： guest 注意都为小写，按下确认键。如果你需要经常配置路由器，可以勾选记住我的密码。

(3) 确定之后则成功登陆路由器配置界面。

如图 为 R2005G 的主界面

4. 系统状态

系统状态显示系统各个方面的状态情况，包括：系统信息、接口信息、主机监控和日志服务。

4.1. 系统信息

状态信息：显示系统运行时间， CPU、内存使用率和活动的主机数

版本信息：显示此产品的产品型号，目前的软件版本和策略库版本信息

网络统计信息：显示各个类型网络累计转发接收包和字节数的统计信息

4.2. 接口信息

接口信息包括： WAN 口的信息以及 LAN 口的信息。

WAN 口

线路类型：显示您目前的连接方式，可以为 PPPoE、 DHCP 或者静态 IP 任意一种方式，具体以 ISP 提供为您的服务为依据显示。

- MAC 地址： WAN 端口的 MAC 地址，此地址由产品出厂时所分配，固定且唯一。
- IP 地址/掩码/网关：您连接上 Internet 后所分配到的 IP 地址，掩码和网关，如无连接时，此处全部显示为 0.0.0.0
- 主 DNS/从 DNS： DNS 地址用于对访问网站时所需要的域名进行解析，输入您最为常用的域名解析服务器地址，也可以由您的 ISP 推荐。如 DNS 不填或错误将无法以 www 的方式访问到网站。
- 备份 DNS：输入首选 DNS 外的另一个备用的 DNS 地址，也可以不填线路状态：如果处于连接状态，则显示连接，如果未连接，则显示已断开。
- 连接时间：显示与 Internet 的连接时间。
- 接收/发送：显示接收/发送包总数。
- 内网线路信息：此选项提供路由器 LAN 端口信息，并列出该端口的 MAC 地址， IP 地址以及接收/发送包总数信息。

4.3. 主机监控

4.3.1 主机监控

LAN 内活动主机数：显示内网里面的主机数

连接数：通俗的解释，一个 IP 的一个端口到外网一个 IP 的一个端口之间的连接， 就是一个连接数。

上行速度/下行速度（B/s）： LAN 内主机的上下行总速度。

上行字节数/下行字节数（B）： LAN 内主机的上下行总字节数。

查看 LAN 主机连接信息：显示 LAN 内主机的信息，包括：主机 IP、连接数、上下行速度、上下行字节数、主机名、在线时间、用户组。

查看：可以查看到此主机 IP 的连接信息

限制：对此主机 IP 内的所有连接端的上下行速度进行限制

4.3.2 主机分析

输入需要查找的 IP 地址，便可查询到目标 IP 主机的各种信息，如：访问控制、 DNS 过滤、MAC 过滤、主机带宽限制、应用优先级等信息。

4.3.3 主机黑白名单

主机黑名单：黑名单中的主机不能访问互联网。

主机白名单：白名单中的主机会无条件通过路由器访问互联网，但会受 QoS、限速的限制。

4.4. 用户信息

可以通过用户信息查看到 PPPOE、 PPTP、 L2TP、 WEB 认证等用户拨号的信息。

4.5. 日志服务

日志服务包括：行为管理日志，系统日志， DDoS 监控信息和网页日志。

行为管理日志：用于记录在开启上网管理功能的“记录” 功能后显示的，只能保留最近一段时间的日志。

记录时间	日志内容
2017-06-27 18:04:24	暴风影音2012 192.168.10.72 00-25-64-D4-69-1F:阻断
2017-06-27 18:00:38	风行 192.168.10.74 B8-AC-6F-B7-7B-5F:阻断
2017-06-27 18:00:17	192.168.10.214 B8-AC-6F-DC-BE-9C访问网址黑名单video.sina.com.cn:阻断
2017-06-27 17:59:25	QQLIVE 192.168.10.74 B8-AC-6F-B7-7B-5F:阻断
2017-06-27 17:59:23	暴风影音2012 192.168.10.72 00-25-64-D4-69-1F:阻断

系统日志：用于记录系统开机时间，以及 WAN 口状态信息（拨号过程、连接状态），以及 WEB 登陆时间等。

记录时间	日志内容
2017-06-27 09:53:29	guest登陆路由器成功
2017-06-27 09:20:04	PPPOE 帐号、密码 认证失败
2017-06-26 16:50:01	guest登陆路由器成功
2017-06-26 15:48:56	PPTP 用户请求断开或连接超时断开
2017-06-26 14:43:02	PPTP 获取IP成功
2017-06-26 14:42:53	PPTP 帐号、密码 认证通过
2017-06-26 08:41:30	PPTP 用户请求断开或连接超时断开
2011-06-26 00:29:41	PPTP 获取IP成功

DDOS 监控信息：用于记录最近一段时间内，疑似内外网 DDOS 类攻击条目，用于辅助分析网络问题。

TCP	源ip不在接口子网内,192.168.2.101:1476->125.39.205.31:443
TCP	黑名单主机发出的包,209.177.82.39:80->58.60.231.106:1075
TCP	黑名单主机发出的包,209.177.82.39:80->58.60.231.106:1075
TCP	黑名单主机发出的包,209.177.82.39:80->58.60.231.106:1075
TCP	黑名单主机发出的包,209.177.82.39:80->58.60.231.106:1075
TCP	黑名单主机发出的包,209.177.82.39:80->58.60.231.106:1075

网页日志：监控主机最近浏览的网页、网页视频、网页下载等信息。

4.6. 网络工具

此功能可以在路由器里 ping 内网或外网地址，用于网络排错、网络分析。

此功能可以在路由器里 tracert 外网地址，用于网络排错、网络分析，了解数据走的路由。

4.7. 接口设置

该功能的位置在网络配置-接口配置里。

此功能用于解决 WAN 口的疑似兼容性问题，如果拨号，或者 WAN 口经常异常，可以选择 10M 全双工试试。

4.8. 抓包设置

通过使用抓包工具抓指定接口的数据包

抓包完成或者停止抓包后，包将存储在 Capture.file 中，导出的文件使用 Wireshark 或 tcpdump 来查看，以供查询分析。

5. 外网接入配置

- 选择外网配置，右侧提供了各种上网类型，请先参照以下说明确定你所用的宽带上网类型，若不清楚你的上网类型可以致电当地宽带运营商询问。
- PPPoE 用户（ADSL）：适用于大多数中国电信、中国联通和中国移动用户。此类用户，通常由一个 Modem（俗称“猫” 或“光猫”），或者直接一条网线接入。没有使用路由器之前的电脑，需要账号和密码，拨号后才能上网。
- 动态 IP 用户（Cable Modem）：一般用于小区宽带、企业、学校内部二级网络等。没用路由器之前，网线直接接电脑就可以自动获取 IP 上网，并且网络配置是“自动获得 IP 地址”和“自动获得 DNS 服务器地址” 。
- 静态 IP 用户：通过指定 IP 地址、网关、子网掩码、 DNS 上网的用户（常见于中大型企业或网吧）。

5.1. WAN 口数量设置

可以通过 WAN 口数量设置扩展或减少 WAN 口数量。

5.2. 外网配置

WAN 口配置的主界面，点击相应操作按钮，进行外网的详细配置界面。

5.2.1 PPPoE 用户(ADSL)设置

在下面的 PPPoE 账户和密码框里里面填入宽带运营商给你上网的用户名和密码。其它设置保持不变，直接点保存生效等待 1 分钟左右即可上网。

工作模式：默认启用 NAT 模式，如果路由模式的话，只能做纯路由，这种方式主要用于运营商，一般用户不要修改；

网络服务商：只用于多线接入情况下，根据具体网络服务商来选择，单线接入时，可以不做任何选择；

线路通断检测：在多线接入时，路由器自动对 WAN 口线路的通断作判断，将断开线路的数据流量切换到其他正常连接的线路上。

线路断线：设置时间段后，在设置时间范围内将接口进行断开处理。

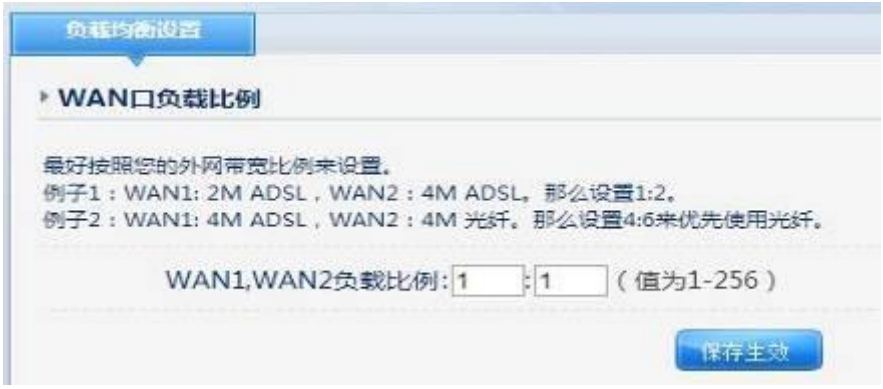
5.2.2 动态 IP 用户(Cable Modem)设置

在“WAN 设置” 里面选择“动态 IP 用户(Cable Modem)” 即可，点击“应用” 。

5.2.3 静态 IP 用户设置

在 WAN 设置里面选择“静态 IP 用户” 用户，将所有原空白的选项都填入宽带运营商分配给您的参数。若不清楚各固定参数的，请询问你的网络维护人员或宽带运营商。

5.3. 负载均衡设置



可以根据各个 WAN 口的带宽来选择负载比例，提高带宽利用率。

举例：如果 WAN1 与 WAN2 口带宽都为 2M，则建议填写 1:1，若 WAN1 为 10M， WAN2 为 2M，则建议填写为 5:1。其余则依次类推。

6. 内网接入配置

路由器作为局域网的网关，这里主要设置路由器的 LAN 口 IP、子网掩码等。

6.1. 内网配置

内网 MAC 配置：可以修改内网的 MAC 地址

内网 IP 地址、子网掩码：为本路由器配置的 LAN 口 IP 地址。默认业务 IP 为 192.168.0.1，子网掩码为 255.255.255.0。请注意局域网中所有计算机的子网掩码必须与路由器掩码一致。

业务 IP：对应路由器 LAN 口一般网络网关

监控 IP：与监控端口对应的监控网段 IP 网关

序列号	IP地址	子网掩码	IP类型	操作
1	192.168.0.1	255.255.255.0	业务IP	
2	192.168.1.1	255.255.255.0	监控IP	

看内网 IP 配置参数：显示内网的 IP 地址和子网掩码以及 IP 的类型。

注意修改内网各业务 IP 时，相应的 DHCP 地址池也需要做相应修改

6.2. DHCP 设置

在左侧菜单中的服务器里可以找到

DHCP 服务器状态：可以选择开启或关闭此功能，开启表示只要网络中的电脑和路由器相连，电脑会自动获取到一个 IP 地址，网关等参数。关闭表示只有电脑设置固定 IP，网关，DNS 等参数才能上网。建议在企业及网吧环境里，选择关闭这个功能，因为开启 DHCP 不仅会导致后面的上网行为管理功能的某些策略难以很好的实现，也对管理内部网络造成困难（难以通过 IP 一一对应人员）。如果选择关闭此功能，请规划好 IP 地址，并正确配置路由器。

DHCP 地址池：默认有两个地址池， 业务地址池 192.168.0.2-192.168.0.254

监控地址池 192.168.1.2-192.168.1.254

可以在服务器地址池子菜单中设置多个地址池，用来限制和规划 DHCP 的内网网段。

在启用中取消勾选，可以相应关闭对应的地址池 DHCP

网关 IP 地址：默认为 LAN 口 IP 为网关，一般不用修改。如果您仅仅把路由器当做一个 DHCP 服务器设备，可以选择你指定的网关 IP。

续租时间：默认分配一个 IP 地址的租期为 1 天，如果您地址池 IP 比较紧缺，可以选择减少租期来缓解，减少不用的 IP 地址。如果您的 IP 足够多，可以把时间延长，减少续约次数。

DNS 代理：默认路由器可以作为 DNS 代理，一般不需改动。如果您内网有单独的 DNS 代理服务器，或者电脑设置的 DNS 都是外网的 DNS，可以不选择。减少路由器压力。但是后果就是如果您的电脑的 DNS 设置为路由器 LAN 口地址， 将不能上网。

DNS 服务器列表：可以填写 3 个 IP，指定分配给电脑的 DNS 地址，建议不用修改。

6.2.1 保留地址

保留地址：用于设置某台电脑，每次自动分配的 IP 地址都为一个固定的 IP 地址，不会被别的电脑占用。输入你想要的名称，以及电脑网卡的 MAC，以及 IP 地址即可完成配置。

6.3. PPPOE 服务器

路由器的 PPPOE 服务器功能，为用户提供一种易于管理的拔号接入方式，特别适用于出租屋等环境，是防止 ARP 病毒或攻击以及 IP 冲突的最好方法。

6.3.1 服务器设置

设置服务器地址及地址池最好使用私有 ip 地址:

(1)10.0.0.1-10.255.255.255

(2)172.16.0.1-172.31.255.255

(3)192.168.0.1-192.168.255.255

6.3.2 账户管理

用于添加 PPPOE 用户

账户名称和密码，就是用户用于拨号的账号与密码。

控制方式可以选择三种，分别是到期时间、可用流量、可用小时，适合不同需求的人群。

账户类型可以选择单用户和多用户，多用户允许一个账号密码可以同时被多人拨号使用。

分配固定 IP：

(1) 多用户模式，分配固定 IP 为该账号的起始地址。

(2) 不要设置为路由器内网口相同网段的私有 ip 地址

注意： 1.多用户模式账户控制中的可用小时数和可用流量为多个用户使用的累加和。

2.分配固定 IP 可设为地址池之外的。

6.4. WEB 认证

Web 认证是一种对用户访问网络的权限进行控制的认证方法，这种认证方式不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行接入认证。当用户需要访问互联网时，必须通过路由器进行认证，只有认证通过后才可以使用互联网资源。如果用户试图通过 HTTP 访问互联网，将被强制访问 Web 认证页面，从而开始 Web 认证过程。

WEB 认证主界面

输入认证页面设置的“提示标题” 与“提示内容”

添加 WEB 认证帐户，并根据需求填写其它选项。

打开浏览器，在弹出的上网认证界面中输入正确的“用户名”与“密码”，点击登录后即可认证成功。

认证成功后，“在线主机”处显示 WEB 认证成功后的在线主机。

6.5. 接入方式管控

(1) 接入方式管控关闭时，默认所有接入方式的主机都访问外网；

(2) 开启此功能后，用户可根据需要选择允许通过路由器的接入方式。

7. 营销 WIFI

微信连 Wi-Fi 是微信推出的快速连接 Wi-Fi 热点的功能，无需输入繁琐的 Wi-Fi 密码，无需进行繁琐的认证过程，只需启用微信客户端即可实现一键上网，同时还能引导用户对公众号的关注。(需要有公众账号才能正常使用)

7.1. 微信连 WFFI 设置

(1) 微信公众账号后台登录 https://mp.weixin.qq.com

(2) SSID、shopID、AppID、SecretKey 到公众账号后台——微信连 WiFi——设备管理——详情中查看，并将对应的内容复制到相应的输入框中即可

注意：开启功能后请勿在其他设置中修改对应 WiFi 的 SSID 或关闭 WiFi，否则微信连 WiFi 功能将会失效

有效期时间：超过认证有效期后需要重新通过微信链接 WIFI。

空闲断线时间：当接入设备下线时长达到已设置的空闲断线时间，将会被清除已认证状态。

强制关注公众账号：用户需要关注您的公众账号才能上网。您需要上传公众的二维码并将生成的 URL 填写至微信公众账号后台。

7.1.2 欢迎设置

店铺名称，输入不超过 15 个字

图片轮播时间

图片设置：单张图片大小不要超过 500KB，支持 JPG、PNG 格式

8. AC 功能：

AC 控制开关：开启关闭 AC 管理功能

9. QoS

当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

9.1. 智能 QoS

9.1.1 智能 QoS

此功能将会自动根据您设置的外网带宽和实时的内网应用情况，调整带宽大小，划分优先级，保证游戏、网页数据的优先转发。

智能 QoS 状态：可以选择开启或关闭。

WAN 线路带宽：以一般 4M ADSL 为例，上行为 0.5M，下行为 4M。如不清楚您的上下行带宽，请咨询您的网络运营商，填写的正确性会直接影响到 QoS 的效果。

WAN 线路预留带宽：系统默认会保留 2%的带宽作为在带宽非常紧张的高峰时期使用，避免网络丢包或延迟。如果您的带宽足够大，且带机量不多，可以把此值调小，相反，则可以适当提高一些。

9.1.2 应用优先级

应用优先级，你可以通过手动配置，将重要应用，如： http smtp pptp 等，加入到高数据转发队列中。 同时将占用带宽较大的，并不重要应用加入到低数据转发队列，从而保证你内网网络高速运行。

优先级：数字越小，优先级越高。

数据转发队列：数字越小，包越先转发。

源主机、用户组：可选择特定的某个 IP，也可选择用户组。如果 2 者均选择，则为 2 者 IP 范围之和。

目的主机：可选择所有主机也可选择特定子网。

协议及端口号：协议可选择所有、 TCP、 UDP、 IGMP 等。模版可选择 HTTP、 IPsec、 FTP、POP3 等。

9.2. 主机带宽控制

本功能可以有效限制主机过分抢占带宽，方便您合理分配有限的带宽资源，防止个别主机过分抢占带宽资源。

未定义主机带宽控制表示在默认情况下，所有内网主机 IP 所独享的最高带宽。

主机带宽控制配置，用于对内网的部分用户组进行单独的带宽配置，可基于时间段控制。

注意 1：这里的速度是 Kbyte（千字节）为单位

注意 2： ADSL 用户，由于上传实际带宽远小于下载带宽，故需要设置小一些。

注意 3：开启智能 QoS 后，不建议开启手工限速。

10. 上网行为管理

上网行为管理的总开关

10.1. 时间段

注意：这里的时间段是生效的时间段。

如上图所示，设置一个上班的时间，勾选星期几，具体时间，点击添加即可。时间段类型可以按周、日或月来进行设置。

10.2. 用户/IP 组

在这里填写组名称，以及 IP 范围，优先级，备注，点击增加即可。

优先级：数字越小优先级越高，“0”为优先级最高，用于在 IP 范围有交叉或重复的时候，决定先满足哪条规则。

10.3. 网址分类管理

作用是禁止、警告、记录对不同类别的网站的访问。目前已经对网站类别进行了细致的划分，你只需要勾选就可实现控制管理。

首先选择你想要控制的用户组（之前配置过），然后勾选启用网址分类管理状态，再选择生效时间，之后选择你想要阻断或控制或警告的网址分类；您可以设置不同用户组的不同权限，比如 A 组 阻断论坛博客， B 组阻断电子购物， C 组警告聊天交友，所有用户记录网络游戏网站等。

阻断表示：无法访问该类主流的网站。

记录表示：在上网行为日志里记录访问的日志。

警告表示：访问该类网站时暂时跳转至警告界面，然后再跳转到要访问的网页上。

10.4. WEB 安全管理

配置 WEB 安全管理可以有针对性的控制用户在浏览网页期间的一些行为。

首先选择你想要控制的用户组（之前配置过），再选择生效时间，在选择是否启用禁用提交，和文件扩展类型过滤，最后保存生效。

禁用提交：勾选即开通该功能,以达到限制用户在网页上提交信息的目的，如论坛的发帖回帖，论坛注册，在网站上登陆账号等。请谨慎使用，可能造成一些网络应用无法正常进行。

文件扩展类型过滤：提供针对某一类型的元素的过滤功能.可以通过该功能过滤所有网络行为中具有相同后缀名的元素。

比如:过滤 flv 格式，添加后，在线视频就无法打开了，但是对优酷、土豆、 6 间房等视频网站仍可进行访问，只是.flv 格式的视频打不开了；

再如 exe ，某些网站会自动下载 exe 文件，添加这个后， exe 文件就无法下载了， swf 则是在网页上常见的 flash 广告条等。

添加 Zip 格式，则无法网站中下载此类型的文件了。

你也可以自己定制一些文件格式。

您可以设置不同用户组的不同权限，比如 A 组过滤 FLV 网址， B 组过滤 ZIP，而 C 组禁用网页提交。

10.5. 代理过滤

支持过滤 Socket4、 5、 HTTP 代理等，用于防止有些用户想通过代理绕过网络限制。你可以选择阻断和记录，记录的意思是记录在日志里，可以在路由器里查看历史记录。

10.6. 聊天软件过滤

针对主流的聊天和即时通讯软件进行阻断和记录，可实现黑白名单功能。

支持主流聊天软件基于用户组、时间段的过滤，您可以设置不同用户组的不同权限，比如 A 组阻断 QQ， B 组阻断飞信，而 C 组全部记录。

实现此项功能，必须启用聊天软件过滤状态

10.6.1 QQ 黑白名单

QQ 黑白名单可以通过具体的 QQ 号码来实现过滤和允许。

只要按下上图中光标所指的 + 号键，在弹出的窗口中，输入 QQ 号码，然后点击右上方的勾。

黑名单表示不能登录的账号，白名单表示不受限制的账号。

10.6.2 QQ 登陆记录

这个功能可以显示当前网络中所有登陆的 QQ 号。你可以通过点击此 QQ 号与之进行对话。

10.7. 股票软件过滤

对部分主流股票软件进行过滤

支持主流股票软件基于用户组、时间段的过滤，您可以设置不同用户组的不同权限。实现此项功能，必须启用股票过滤状态。

10.8. P2P 软件过滤

实现阻断、记录主流的 P2P 类的下载软件。

支持主流 P2P 软件基于用户组、时间段的过滤，您可以设置不同用户组的不同权限。实现此项功能，必须启用 P2P 过滤状态。

10.9. 视频软件过滤

该功能主要实现过滤、记录主流的在线视频类软件。

支持主流视频软件以及视频网站的基于用户组、时间段的过滤，您可以设置不同用户组的不同权限。实现此项功能，必须启用视频软件过滤状态。

10.10. 邮件监控

选择您要监控的用户组，并启用邮件监控状态，选择时间后，填写您或老板的邮箱地址，点击保存。之后指定用户使用 Foxmail 发送的 E-mail 将会复制一份到指定邮箱。

此功能请谨慎使用

(1) 可能涉及他人隐私，请三思后考虑是否使用。

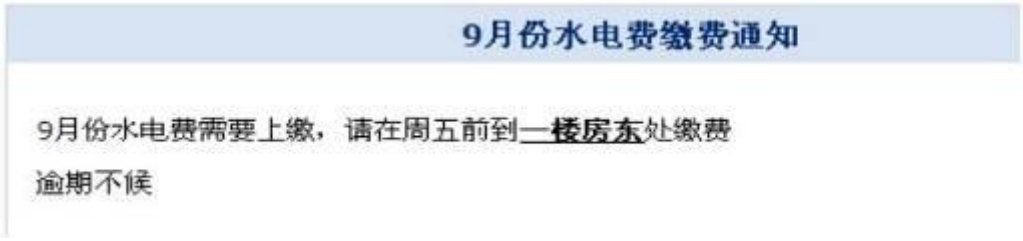
(2) 监控邮件过多时可能堵塞指定的邮箱。

10.11. 电子公告

用于向内网发布通告信息，在指定时间段内通过网页的形式告知内网用户。

先编辑电子公告内容

在制定时间内，设置出现频率，设置公告的对象。



电子公告的效果

11. 网络安全

11.1. 攻击防御

这里提供常见的一些攻击防御功能

攻击防御：建议用于在内外网收到攻击频繁下的环境开启。

禁止 LAN 到 LAN 的包：用于隔离不同网段的数据包。

禁止 WAN 口响应 ping 包：从外网 ping 路由器的 WAN 口地址， 路由器不作回应，现象也就是 ping 不通，防止黑客的大规模扫描 IP。

11.2. 访问控制

访问控制，对指定的源、目的主机的协议及端口在固定时间段的有效控制。

IP 互联网访问控制状态为启用时，您所做的设置才会生效。

举例：现增加源主机（特定主机）： 192.168.1.2，目的主机：所有主机，应用模板：所有模板（请选择模板则表示所有模板），协议及端口： ALL，在启用“IP 互联网访问控制状态”的情况下，如果选择了禁止，则 IP 为 192.168.1.2 的主机可以上网；如果定义“禁止”，则只有 IP 为 192.168.1.2 的主机不可以上网。

11.3. IP/MAC 绑定

该功能用于 IP 和 MAC 地址的绑定，作用是防止用户乱改 IP，防止 IP 冲突，防御 ARP 病毒等。

IP 地址：该用户的内网固定 IP 地址

MAC 地址：用户网卡的 MAC 地址

备注：可以写这个 IP 的对应人

ARP 攻击防御： ARP 攻击防御能有效地防御内网的 ARP 攻击监控

11.3.1 ARP 监控

此功能可以显示路由里的 ARP 表，最右侧可以选择绑定和取消绑定，最下面有全部绑定的功能，不需要一条条的绑。

11.4. DNS 过滤

要实现此功能必须先启用 DNS 过滤

你可以选择允许还是禁止表外的数据通过路由器。

允许表外数据通过路由器，表示在规则以外的上网数据也是可以通过路由的。

禁止表外的数据通过路由器，表示在规则以外的上网数据是不能通过路由的。

DNS 过滤可以对域名解析服务进行过滤。例如：对 www.sina.com.cn 过滤，在首 DNS 过滤状态设为启用，缺省过滤规则为允许，添加规则中的过滤关字输入 sina，状态选择禁止。这样就可以禁止访问 www.sina.com.cn 了。

11.5. MAC 地址过滤

要实现此功能必须先启用 MAC 过滤

你可以选择允许还是禁止表外的数据通过路由器。

允许表外数据通过路由器，表示在规则以外的上网数据也是可以通过路由的。

禁止表外的数据通过路由器，表示在规则以外的上网数据是不能通过路由的。

这里可以选择是手动添加 MAC 地址，还是从路由器的 ARP 表中读取 MAC，你可以把某个或者某些 MAC 地址添加到禁止列表中，这样，这些电脑就不能上网了。

12. VPN

这里提供的是 VPN（PPTP）服务端功能，主要目的是让出差、或是异地的人员可以访问总部的内网资源，甚至使用公司的出口来上网。配置完毕后，使用操作系统自带的 VPN 拨号连接即可使用。

12.1. PPTP 客户端

此功能用于连接其他 VPN 服务端设备

状态：选择启用， PPTP 客户端下方的配置才会生效

服务器地址：可以选择 IP 或者域名。在后面框中填入要连接的 PPTP 服务器端 WAN 口的静态 IP 地址或者域名。

服务器端口：输入对应的域名端口号。

用户名：输入要连接的 PPTP 服务器端设置的用户名

密码：输入要连接的 PPTP 服务器端设置的密码

数据加密：如果服务器端加密，这里必须加密。

NAT：默认为启用 NAT，非专业人士请不要修改。

模式：可以选择 ISP 模式或者企业模式。

ISP 模式指的是在远程网络上使用默认网关，代理内网用户访问 Internet。

企业模式指的是通过 PPTP 隧道实现在隧道两端企业内网互访。

需要注意的是，如果选择了企业模式，做为 PPTP 服务器端的路由器在设置用户时一定要填写网络地址和掩码，否则无法连接成功。

12.2. PPTP 服务器

可以选择启用或者禁止 PPTP 服务，如果想启用 PPTP 服务，需要填写 PPTP 服务端地址（可默认），客户端地址（可默认），设置最大 PPTP 连接数。数据加密为默认设置（与操作系统默认设置相同）

12.2.1 PPTP 用户

使用 PPTP，需要输入用户名和密码来连接到 PPTP 服务器。

网络地址为选填：设置该账号的内网地址，用于服务端路由器下的电脑也能访问客户端的网络资源。

12.2.2 PPTP 状态

显示连接 PPTP 的用户名，接入 IP 地址以及分配的 IP 地址。

12.3. L2TP 客户端

状态：选择启用， PPTP 客户端下方的配置才会生效

服务器地址：可以选择 IP 或者域名。在后面框中填入要连接的 PPTP 服务器端 WAN 口的静态 IP 地址或者域名

用户名：输入要连接的 PPTP 服务器端设置的用户名

密码：输入要连接的 PPTP 服务器端设置的密码

NAT：默认为启用 NAT，非专业人士请不要修改。

模式：可以选择 ISP 模式或者企业模式。

ISP 模式指的是在远程网络上使用默认网关，代理内网用户访问 Internet。

企业模式指的是通过 PPTP 隧道实现在隧道两端企业内网互访。

需要注意的是，如果选择了企业模式，做为 PPTP 服务器端的路由器在设置用户时一定要填写网络地址和掩码，否则无法连接成功。

服务器网段：填写你所需要连接 VPN 的对端子网。

服务器掩码：填写你所需要连接 VPN 的对端子网掩码。

L2TP 客户端状态将显示所连接 VPN 的连接状态。

12.4. L2TP 服务器

可以选择启用或者禁止 L2TP 服务，如果想启用 L2TP 服务，需要填写 L2TP 服务端地址（可默认），客户端地址（可默认），设置最大 L2TP 连接数。 可选择 IPsec 封装（密码在 IPSec 设置下的 Rsa 密钥获取到，也可以手动填写预共享密码）。

12.4.1 账户管理

使用 L2TP，需要输入用户名和密码来连接到 L2TP 服务器。

网络地址为选填：设置该账号的内网地址，用于服务端路由器下的电脑也能访问客户端的网络资源。

12.4.2 L2TP 状态

显示连接 L2TP 的用户名， 连接状态， 接入 IP 地址以及分配的 IP 地址。

12.5. IPSec 设置

状态：选择启用， IPSec 下方的配置才会生效。

认证模式：选择 PSK 模式则填写预共享密码。选择 Rsa 则在右边 Rsa 密码设置里面点击生成。

模式：选择服务器模式则客户端是选择安装 IPSec 客户端软件连接。选择对等模式则对端是选择用路由器，来连接 IPSec。

外出接口：选择你连接 IPSec 的 WAN 口。

对端 IP 地址：选择对端连接 IPSec 的 WAN 口公网 IP 地址。

本地子网：填写路由器 LAN 口网段及子网掩码。

对端子网：填写对端路由器 LAN 口网段及子网掩码。

协商模式：选择主动模式，默认即可。

通道模式：选择隧道模式，默认即可。

阶段一/阶段二：选择加密认证算法，需与对端设置一致才可连接。

协议：协议为 ESP 时，支持加密且能适应本端到对端之间存在 NAT 的情况，推荐使用。协议为 AH 认证时，数据包不会加密，仅提供 IP 和数据报文未被修改的保证。

12.5.1 RSA 密码设置

如 IPSec 设置里选择了 RSA 认证模式，则可在此处点击生成密码。

12.5.2 IPSec 状态

此处将显示 IPSec 的连接状态，如本地 IP、对端 IP 等。

12.5.3 IPSec 日志

此处功能可用于查看 IPSec 连接具体阶段情况。是否成功连接，以及出现的问题在级阶段。

13. 高级设置

13.1. 虚拟服务

此功能用来实现通过互联网上访问企业内部主机的某些应用和服务。比如：通过端口的映射，你可以架设 WEB 服务器，实现远程访问内网等功能。

你需要先给这个规则起一个名称，可以中文也可以是英文。

第二步填写你内部需要做这个服务的主机 IP 地址。

第三步选择外部端口的协议和端口号（TCP 还是 UDP 取决于你这个程序，外部端口号可以自己选择，也可以和内部端口一样）

第四步填写内部端口，内部端口指的是主机这个服务或应用所使用到的端口。

举例：一个监控服务器用到的端口是 TCP 的 12345 端口，服务器的 IP 是 192.168.10.110，那么外部端口你可以设为 12345，也可以设置其他端口，比如 80，或者 8080，到时你在外网访问的时候后面跟着你设置的外部端口就可以了。

13.2. 静态 NAT

静态 NAT 时将内网主机 IP 和外网 IP 地址做地址转换，实现 DMZ 功能。

静态 NAT 的外网地址是 ISP 分配给你的公网 IP 地址，通常和该线路 WAN 口 IP 地址在同一个网段。

13.3. 动态域名

动态域名主界面，点击“操作” 按钮进行各 WAN 口动态域名配置。

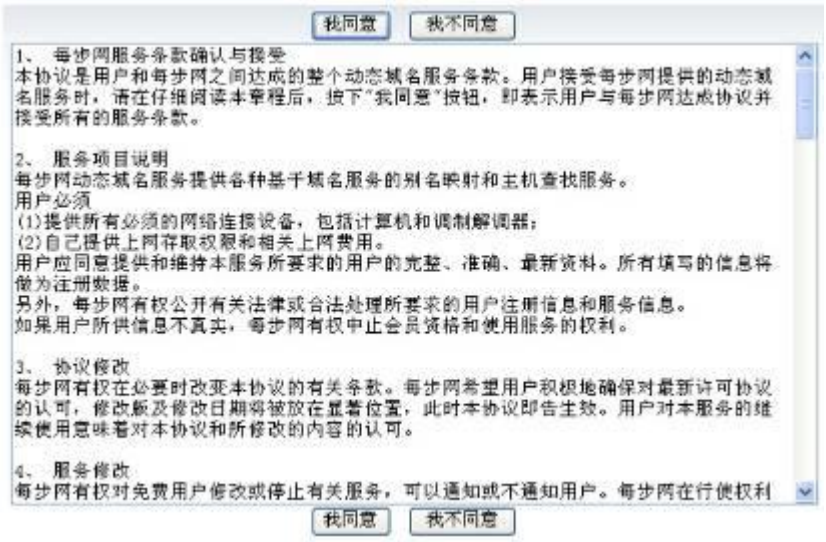
动态域名解析服务是将一个动态变化的 IP 地址（如 ADSL 拨号上网）解析成固定的域名的一种服务。只需输入你所注册的域名，即可远程访问路由器，同时这项功能对于你在你的私有网络中架设 FTP 和 WEB 服务器是非常有用的。使用前，需向 DDNS 服务提供商申请这项服务。目前支持花生壳、每步、希网的 DDNS。

动态域名的申请

下面以“每步（www.meibu.com）”为例，简单介绍一下申请 DDNS 的过程：

进入“每步（www.meibu.com）”网站

点击圈中所示“》现在加入”，进行免费域名申请。



点击“我同意”，进入申请免费域名的资料填写。

“提交” 后，域名即申请成功。

请按照以下步骤使用 DDNS 服务：

访问： www.meibu.注册免费域名，您可以得到一个帐户

输入在 DDNS 提供商处注册有效的用户名和密码

点击启用后并保存 DDNS 的设置。动态域名服务(DDNS)设置完成后，即可通过该域名访问本路由器。

可以在局域网计算机的命令提示行状态下，使用 Ping 命令（例如： ping xxx.dyndns.org）检查动态域名解析服务是否生效。看到正确解析出 IP 地址（例如： 202.104.237.179），证明域名解析正确。

```
C:\>ping www.neibu.com

Pinging xxx.dyndns.org [202.104.237.179] with 32 bytes of data:

Reply from 202.104.237.179: bytes=32 time<1ms TTL=255

Reply from 202.104.237.179: bytes=32 time<1ms TTL=255

Reply from 202.104.237.179: bytes=32 time<1ms TTL=255

Reply from 202.104.237.179: bytes=32 time<1ms TTL=255

Ping statistics for 202.104.237.179:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

13.4. 策略路由

根据需要求对指定的源和目的主机的端口或指定应用模板在固定时间段指定出口策略，源主机可以选择为用户组。

注意： 配置规则存在重复的只会匹配优先级高的。

13.5. 静态路由

类型： 分为 NET 与 HOST， NET 表示此条静态路由到达目的为网络位址， HOST 表示此条静态路由到达目的为主机位址。

目的地址： 目的主机的 IP 地址或目的网络的 IP 地址

掩码：目的地址的子网掩码

网关： 下一跳路由器入口的 IP 地址。

在路由表中，选中某个静态路由，单击右下角的“删除” 按钮，即可删除静态路由。

非专业人士请不要配置。

13.6. DMZ

DMZ 配置主界面，点击“操作” 按钮，进行各 WAN 口的 DMZ 配置。

DMZ：非军事化区，用与把某台电脑或某个服务器的全部端口完全暴露在公网上，不受路由 NAT 隐藏等约束，缺点是会给 DMZ 主机带来安全隐患，建议不要长期使用。

13.7. UPNP

UPNP：通用即插即用协议，通俗的说就是配合应用程序来自动做端口映射。

常用于 P2P 程序，某些办公系统等。拿 E-mule 来说，使用这个功能后就可以获得更高的速度。

最大允许创建 UPNP 条目：默认总共的条目 10 条，如果需要增加可以自定义，但是条目过多会给路由器带来更多负载。

UPNP 条目配置：这里用来指定主机 IP 所能够创建的 UPNP 条目。你也可以对某些 IP 关闭 UPNP 功能，在状态里选择禁止即可。

13.8. 端口镜像

端口镜像是把通过被捕获端口的数据包抄送一份发到捕获端口，方便管理员分析通过路由器数据。

13.9. 组规则

组规则是针对 在 PPPoE、web 认证等账户设置处选择此处授权组规则，这样您可以实现依据账户的策略授权。

设置好的策略组可在设置 PPPOE、 WEB 认证设置时提供选择，方便快捷。

14. 系统工具

14.1. 管理选项

14.1.1 用户名密码

用户名密码：这里指的是登陆路由器配置的账号密码，拥有这个账号密码才有权限配置路由。

注意：用户名和密码默认均为 guest，强烈建议更改为一个比较安全的账号密码。如果不更改，则可能导致路由设置被非法篡改，网络出现异常等情况。请牢记您的密码。至此路由器的一些基本设置就完成了，你已经可以轻松上网了。

14.1.2 WEB 端口管理

该功能可以更改本地访问时的端口，以增加安全性。默认是 80 端口。

比如你更改为 8087 端口，那么你在本地访问的时候就应该这样：在浏览器里输入： http：// 路由内网 IP 地址:8087 。

14.1.3 WEB 远程管理

如果你需要在外网访问这个路由器，则必须启用 WEB 远程管理，端口号你可以自定义。如果你开启了远程管理，那么密码一定要足够安全，避免黑客篡改。

14.2. 时间设置

此功能是设置路由器的时间的，可以选择从网络上自动获取，也可以手动配置时间。注意路由器断电后不会保存时间。

14.3. 参数备份/导入配置

参数备份：此功能可以把路由器的配置信息保存下来。

参数恢复：此功能可以吧备份好的文件恢复到路由器里。

注意：不同版本的固件之间参数恢复可能有兼容问题，这种情况建议不要跨版本使用。

14.4. 软件升级

此功能用于升级路由器的固件，可以解决一些 bug，或提高一些性能，或增加一些功能。点击浏览，选择固件，然后点击升级即可。升级后，建议恢复默认，然后重新配置一遍。

该功能用于恢复出厂时设置的参数。

立即重启：该功能用于重新启动路由器，期间会丢包，重启时间大约为 15 秒钟。

定时重启：该功能用于定时重新启动路由器，比如启用后，设置每天 00:00 定时重启。

至此，可以访问隔离口下的网络设备